

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-39158

(43)公開日 平成11年(1999) 2月12日

(51)Int.Cl.⁶

G 0 6 F 9/06
12/14

識別記号

5 5 0
3 1 0

F I

G 0 6 F 9/06
12/14

5 5 0 Z
3 1 0 Z

審査請求 未請求 請求項の数 8 F D (全 8 頁)

(21)出願番号

特願平9-210006

(22)出願日

平成9年(1997) 7月18日

(71)出願人 000004226

日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(71)出願人 591230295

エヌティティエレクトロニクス株式会社
東京都渋谷区桜丘町20番1号

(72)発明者 河久保 秀二

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 高田 俊介

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 弁理士 川久保 新一

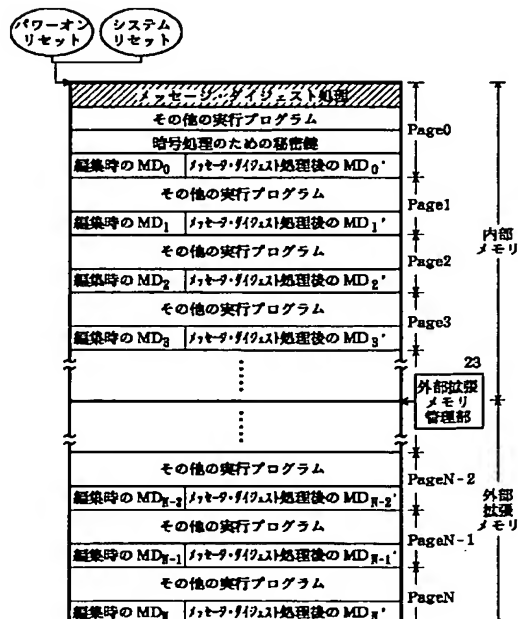
最終頁に続く

(54)【発明の名称】 実行プログラムの保護方法およびその装置

(57)【要約】

【課題】 1チップの中にFROM (フラッシュメモリ) 等のROMとRAMと処理部とが複合して構成されているLSIにおいて、処理装置自身の秘密情報(秘密鍵)の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を提供することを目的とするものである。

【解決手段】 パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。



【特許請求の範囲】

【請求項 1】 パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出段階と；上記改竄検出段階において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止段階と；を有することを特徴とする実行プログラムの保護方法。

【請求項 2】 請求項 1 において、

上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み段階を有し、

上記改竄検出段階は、

上記実行プログラムを暗号処理する暗号処理段階と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第 2 のメッセージ・ダイジェストを抽出する第 2 のメッセージ・ダイジェスト抽出段階と；上記第 2 のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合段階と；上記メッセージ・ダイジェスト照合段階において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定段階と；によって構成されていることを特徴とする実行プログラムの保護方法。

【請求項 3】 請求項 2 において、

上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれていることを特徴とする実行プログラムの保護方法。

【請求項 4】 パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と；上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；を有することを特徴とする実行プログラムの保護装置。

【請求項 5】 請求項 4 において、

上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段を有し、

上記改竄検出手段は、

上記実行プログラムを暗号処理する暗号処理手段と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第 2 のメッセージ・ダイジェストを抽出する第 2 のメッセージ・ダイジェスト抽出手段と；上記第 2 のメッ

セージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と；上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と；によって構成されていることを特徴とする実行プログラムの保護装置。

【請求項 6】 請求項 5 において、

上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれていることを特徴とする実行プログラムの保護装置。

【請求項 7】 パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と；上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項 8】 所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段と；上記実行プログラムを暗号処理する暗号処理手段と；上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第 2 のメッセージ・ダイジェストを抽出する第 2 のメッセージ・ダイジェスト抽出手段と；上記第 2 のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と；上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と；上記改竄判断手段において上記改竄が判断されると、上記実行プログラムの実行を直ちに停止する実行停止手段と；としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、実行プログラムを保護する方法およびその装置に関する。

【0002】

【従来の技術】従来、パーソナルコンピュータや、パーソナルコンピュータの拡張バスに画像処理・音声処理等の専用制御ボード等が接続され、上記専用制御ボード等において、これらの処理や制御を実行する CPU と、プログラムの実行メモリ（RAM）と、実行プログラムの保管や処理開始時や実行中に読み出し／書き込みされるデータメモリ（ROM）とが、互いに別々に構成され、バスによって接続される構成が採用されている。

3

【0003】上記構成においては、上記実行メモリ、上記データメモリの内容を、実行プログラムの実行前に、部分的に変更することが可能である。したがって、実行メモリ、データメモリの内容を、実行プログラムの実行前に、第三者が部分的に変更すれば、上記実行プログラムの実行する処理装置自身の秘密情報（秘密鍵）を読み出すことが可能であり、また、上記処理装置における意図しない動作を、第三者が外部から強制的に実行させることが可能である。

【0004】

【発明が解決しようとする課題】図5は、従来の画像処理・音声処理等の専用制御ボードCB1を示すブロック図である。

【0005】画像処理・音声処理等の専用制御ボードCB1は、処理部（CPU）11と、データメモリとしてのROM12と、実行メモリとしてのRAM13とを1チップに封入したものである。なお、符号14は、インタフェース部であり、符号15は、カードI/F部である。

【0006】このように、実行メモリとデータメモリと処理部とを1チップ化することによって、上記処理装置自身の秘密情報（秘密鍵）が伝送される信号線は、上記チップの外部に露出しないので、第三者が、チップの外部において、信号線に端子等を接触させ、上記秘密情報（秘密鍵）を取り出す操作を実行することは不可能である。

【0007】つまり、上記の場合、信号線に端子等を接触させ、上記秘密情報（秘密鍵）を取り出す操作を実行するためには、チップのケースを開く必要があり、そのケースを開いたとしても、チップ内部の配線のうちでの配線に端子等を接触させればよいかの判断が極めて困難であり、また、端子等を接触させるべき配線が分かったとしても、チップ内部の微細な配線に端子等を接触させることが實際上不可能である。したがって、上記処理装置自身の秘密情報（秘密鍵）の読み出しを阻止することができ、また、外部からの悪意による処理装置の意図しない動作を阻止することができる。

【0008】しかし、上記のように1チップ化したとしても、RAM13の内容をコピーすれば、上記処理装置自身の秘密情報の読み出しを阻止することができないという問題がある。

【0009】また、上記のように1チップ化したとしても、製造工程で用いるROM書き込み装置を利用して、ROM12の内容を改竄した場合や、RAM13を部分修正した場合には、外部からの悪意による処理装置の意図しない動作を阻止することができないという問題がある。

【0010】本発明は、1チップの中にFROM（フラッシュメモリ）等のROMとRAMと処理部とが複合して構成されているLSIにおいて、処理装置自身の秘密

4

情報（秘密鍵）の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる実行プログラムの保護方法およびその装置を提供することを目的とするものである。

【0011】

【課題を解決するための手段】本発明は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出し、この改竄検出において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止するものである。

【0012】

【発明の実施の形態および実施例】図1は、本発明の一実施例である実行プログラムの保護装置PP1を示すブロック図である。

【0013】実行プログラムの保護装置PP1は、CPU等で構成されている処理部21と、データメモリとしてのROM22と、実行メモリとしてのRAM23と、インタフェース部14と、カードI/F部15と、拡張ROM24と、拡張RAM25と、外部拡張メモリ管理部26とを有するものである。

【0014】また、実行メモリとしてのRAM23と、データメモリとしてのROM22と、処理部21と、インタフェース部14と、外部拡張メモリ管理部26とは、図1において太線で囲まれており、この太線内の素子が1チップ化されている。

【0015】処理部21は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段の例であり、上記改竄検出段階において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段の例である。また、処理部21は、上記所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段の例である。

【0016】なお、「メッセージ・ダイジェスト」は、メッセージ・ダイジェストの対象となる原文（上記実施例においては、実行プログラム）が1ビットでも書き換えられると、その原文についてメッセージ・ダイジェスト処理を実行した後に、変化するものである。

【0017】さらに、上記改竄検出手段は、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第2のメッセージ・ダイジェストを抽出する第2のメッセージ・ダイジェスト抽出手段と、上記第2のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上

記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成され、これらの各手段も、処理部 21 が実現する。なお、上記編集時のメッセージ・ダイジェストは、上記暗号処理を実行しても変化しない態様で書き込まれている。

【0018】ここで、「メッセージ・ダイジェスト」は、上記実施例においては、一方向性ハッシュ関数によって実行プログラムを処理した後における最後の 16 バイトのデータであり、「メッセージ・ダイジェスト処理」は、一方向性ハッシュ関数によって実行プログラムを処理する動作である。上記一方向性ハッシュ関数のアルゴリズムとしては、MD2、MD5、SHA-1 等があり、これらのうちのどのアルゴリズムを使用してもよい（MD2、MD5、SHA-1 については、「『暗号理論入門』 岡本栄司著 共立出版株式会社」を参照）。また、上記一方向性ハッシュ関数以外の関数を使用して実行プログラムを処理することによって、メッセージ・ダイジェストを実現するようにしてもよい。

【0019】図 2 は、上記実施例におけるメモリマップを示す図である。

【0020】図 2 に示すメモリマップは、RAM 23 の内部メモリの領域と、拡張 RAM 25 の外部拡張メモリの領域とが使用され、Page 0 ~ Page N で構成されている。

【0021】Page 0 には、メッセージ・ダイジェスト処理のプログラムと、その他の実行プログラムと、暗号処理のための秘密鍵と、Page 0 に関する編集時のメッセージ・ダイジェスト MD₀ と、Page 0 に関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェスト MD₀' とが格納されている。

【0022】なお、メッセージ・ダイジェスト処理する場合、上記のように、MD2、MD5、SHA-1 等のうちのどのアルゴリズムを使用してもよいが、所定 Page について編集時のメッセージ・ダイジェストを生成する場合に使用するアルゴリズムと、所定 Page について実行プログラムを走行させる前にその Page おいてメッセージ・ダイジェスト処理する場合に使用するアルゴリズムとが同一である必要がある。

【0023】Page 1 には、その他の実行プログラムと、Page 1 に関する編集時のメッセージ・ダイジェスト MD₁ とが格納されている。また、メッセージ・ダイジェスト処理後には、Page 1 に関するメッセージ・ダイジェスト処理後のメッセージ・ダイジェスト MD₁' が、Page 1 に格納される。

【0024】Page 2 以降の各 Page には、Page 1 における内容と同様の内容が格納され、その他の実行プログラムと、その Page に関する編集時のメッセージ・ダイジェストとが格納され、また、メッセージ・ダイジェスト処理後には、その Page に関するメッセージ・ダイジェスト処

理後のメッセージ・ダイジェストが、その Page に格納される。

【0025】なお、メッセージ・ダイジェスト処理は、アルゴリズムを明示しないメッセージ・ダイジェスト処理であり、各 Page のメッセージ・ダイジェストを作成する機能を有し、Page 0 のメッセージ・ダイジェスト処理は、各 Page のメッセージ・ダイジェストをとる。つまり、図 2 には、Page 0 にのみメッセージ・ダイジェスト処理が記載されているが、Page 1 以降の各 Page においてメッセージ・ダイジェスト処理が実行される。

【0026】また、「実行プログラム」は、たとえば電文を外部から読み込む処理や、その読み込んだ電文に暗号処理を施す処理を記述したプログラムである。さらに、「その他の実行プログラム」は、メッセージ・ダイジェスト処理のプログラム以外の実行プログラムである。

【0027】次に、上記実施例の動作について説明する。

【0028】図 3 は、上記実施例において、実行プログラムの保護装置 PP1 を製造するときにおける動作を示すフローチャートである。

【0029】まず、Page の関数 n を「0」とし（S1）、Page n に書き込むべき実行プログラムをロードする（S2）。そして、編集時のメッセージ・ダイジェスト MD _{n} を生成し（S3）、上記編集時のメッセージ・ダイジェスト MD _{n} を、該当 Page の最後の 16 バイトに書き込む（S4）。

【0030】次に、Page n に書き込むべき実行プログラムについてメッセージ・ダイジェスト処理を実行することによってメッセージ・ダイジェスト MD _{n} ' を生成し（S5）、1 Page 分のプログラムをメモリ 23 に書き込み、その書き込まれた内容を編集する（S6）。そして、編集された内容を Page 単位で PROM 22 に書き込み（S7）、次の Page について上記処理（S2 ~ S7）を実行し（S8、S9）、最大の Page N まで上記処理（S2 ~ S7）が終了すると、実行プログラムの保護装置 PP1 を製造する場合における全ての処理を終了する。

【0031】次に、上記実施例における実行プログラムの保護動作について説明する。

【0032】図 4 は、上記実施例における実行プログラムの保護動作を示すフローチャートである。

【0033】まず、電源投入時にパワーオンリセットする（S11）か、または、システムリセットした（S12）後に、内蔵の ROM / PROM 22 のリセット・エントリ・アドレスに分岐し、メッセージ・ダイジェスト処理を実行する（S21）。なお、各処理の最後に得られるデータ 16 バイトに、上記メッセージ・ダイジェスト MD' を割り当てる。

【0034】編集時のメッセージ・ダイジェスト MD

10

20

30

40

50

7

と、実行プログラムを走行する毎に、その直前にメッセージ・ダイジェスト処理が行われたメッセージ・ダイジェストMD'とを、照合手段(図示せず)が照合する(S22、S24～S31)。そして、この照合の結果、上記予め作成されている編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが、全てのPageにおいて一致した場合にのみ、上記実行プログラムの動作を通常通りに開始させる。

【0035】すなわち、実行プログラムに変化が加えられていなければ(改竄されていなければ)、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'が変化しないので、このメッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'は、編集時のメッセージ・ダイジェストMDと同じである。

【0036】一方、上記照合の結果、編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合(S22、S24、S32)、実行プログラムが変化されている場合であり、多くの場合、その実行プログラムが改竄されているので、その段階で、実行プログラムの実行を停止する。編集時のメッセージ・ダイジェストMDと、メッセージ・ダイジェスト処理後のメッセージ・ダイジェストMD'とが一致しなかった場合、その実行プログラムが改竄されたと判断し、その後の実行プログラムの実行を停止する。

【0037】このようにすることによって、1チップの中にFROM(フラッシュメモリ)等のROMとRAMと処理部とが複合して構成されているLSIにおいて、実行プログラムが改竄されたと判断されると、その後の実行プログラムの実行を停止するので、処理装置自身の秘密情報(秘密鍵)の読み出しを阻止することができ、また、悪意による処理装置の意図しない動作を阻止することができる。

【0038】実行プログラムが大規模であれば、上記実施例のように外部拡張メモリを使い、この場合、命令によって、メモリ拡張モード・レジスタを設定する。このようにすることによって、外部メモリ領域に外部デバイスを接続できる外部拡張モードになる。

【0039】上記実施例において、実行プログラムが大規模でなければ、拡張ROM24、拡張RAM25、外部拡張メモリ管理部26を省略するようにしてもよい。

【0040】上記実施例を、装置の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段とを有する実行プログラムの保護装置である。

8

【0041】この場合、所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段を有し、上記改竄検出手段は、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第2のメッセージ・ダイジェストを抽出する第2のメッセージ・ダイジェスト抽出手段と、上記第2のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段とによって構成されている。

【0042】また、上記実施例を、記録媒体の発明として把握すると、上記実施例は、パワーオンリセット後またはシステムリセット後であって、所定の実行プログラムが走行する前に、上記実行プログラムが改竄されていることを検出する改竄検出手段と、上記改竄検出手段において上記改竄が検出されると、上記実行プログラムの実行を直ちに停止する実行停止手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【0043】この場合、所定の実行プログラムを編集し、この編集された実行プログラムのメッセージ・ダイジェストである編集時のメッセージ・ダイジェストを所定のメモリに書き込む編集時のメッセージ・ダイジェスト書き込み手段と、上記実行プログラムを暗号処理する暗号処理手段と、上記暗号処理された実行プログラムの中から、メッセージ・ダイジェスト処理されたメッセージ・ダイジェストである第2のメッセージ・ダイジェストを抽出する第2のメッセージ・ダイジェスト抽出手段と、上記第2のメッセージ・ダイジェストと、上記編集時のメッセージ・ダイジェストとを照合するメッセージ・ダイジェスト照合手段と、上記メッセージ・ダイジェスト照合手段において照合が得られなかったときに、上記実行プログラムが改竄されていると判断する改竄判定手段と、上記改竄判定手段において上記改竄が判断されると、上記実行プログラムの実行を直ちに停止する実行停止手段ととしてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体である。

【0044】

【発明の効果】本発明によれば、1チップの中にFROMとRAMと処理部とが複合して構成されているLSIにおいて、処理装置自身の秘密情報の読み出しや、悪意による処理装置の意図しない動作を排除することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施例である実行プログラムの保護装置PP1を示すブロック図である。

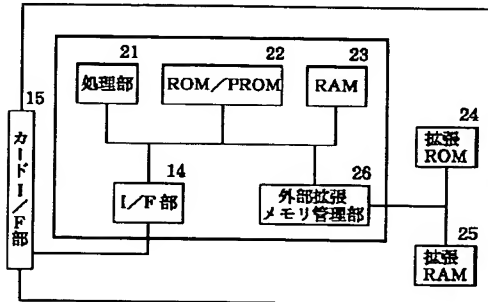
【図2】上記実施例におけるメモリマップを示す図である。

【図3】上記実施例において、実行プログラムの保護装置PP1を製造するときにおける動作を示すフローチャートである。

【図4】上記実施例における実行プログラムの保護動作のフローチャートである。

【図1】

PP1: 実行プログラムの保護装置



K4144

【図5】従来における画像処理・音声処理等の専用制御ボードCB1を示すブロック図である。

【符号の説明】

PP1…実行プログラムの保護装置、

21…処理部、

22…ROM/PROM、

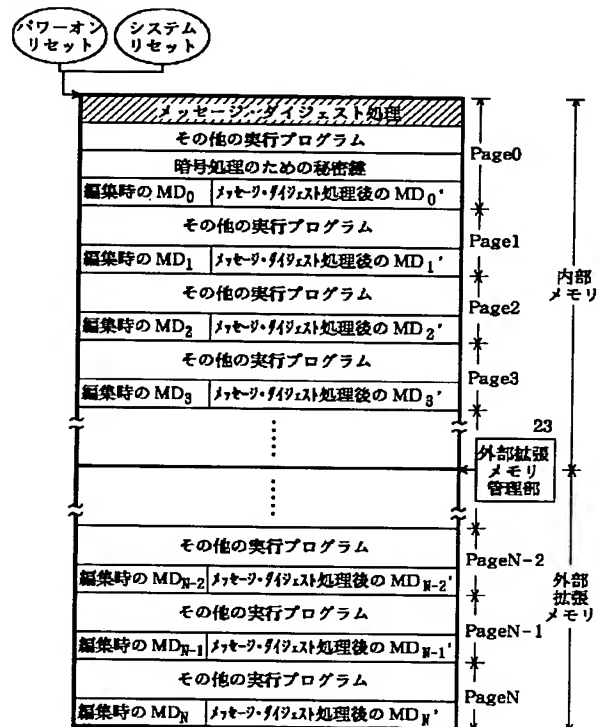
23…RAM、

24…拡張ROM、

25…拡張RAM、

10 26…外部拡張メモリ管理部。

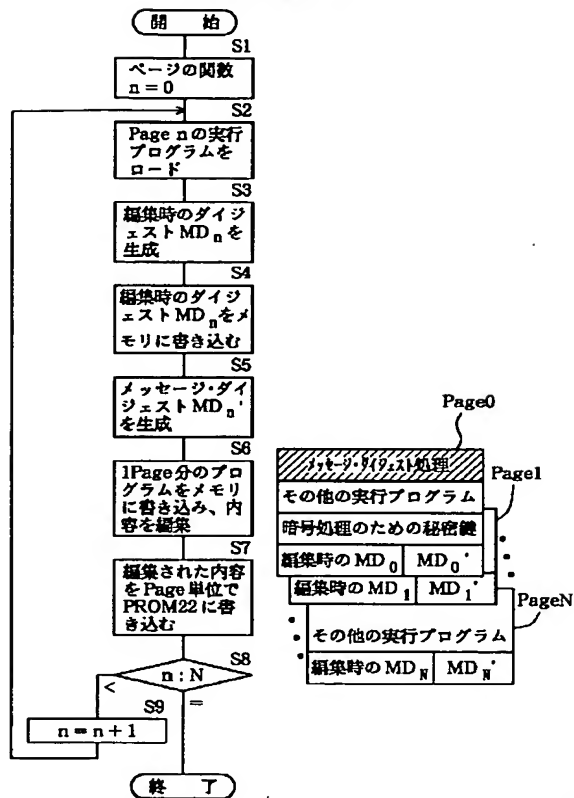
【図2】



K4144

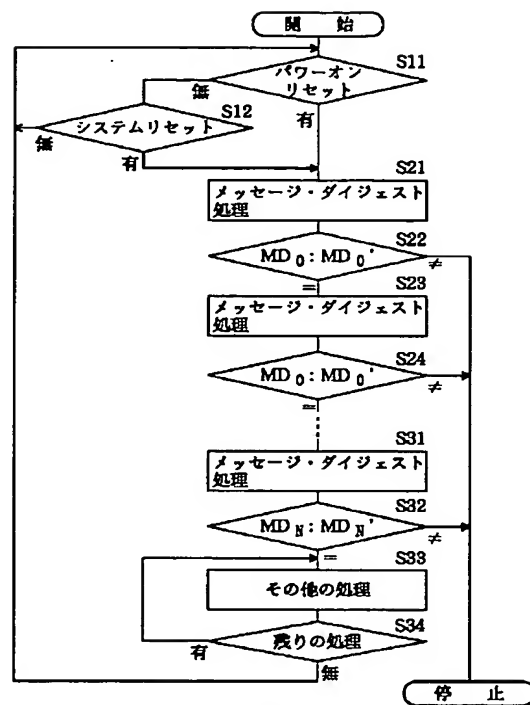
【図3】

製造時の処理手順



K4144

【図4】



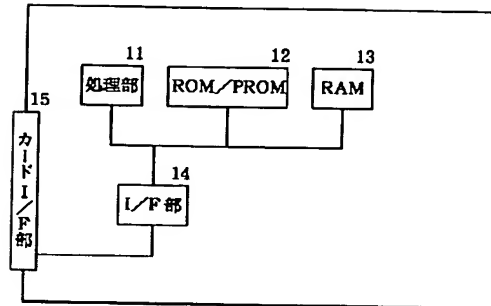
MD_n : Page n についての編集時のメッセージ・ダイジェスト
(ROM/RAM22に実行プログラムから書き込まれた
ときのメッセージ・ダイジェスト)

MD_n^{*} : Page n に関するメッセージ・ダイジェスト処理後の
メッセージ・ダイジェスト

K4144

【図5】

CB1: 従来の専用制御ボード



K4144

フロントページの続き

(72)発明者 山中 喜義

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 松本 博幸

東京都渋谷区桜丘町20番1号 エヌティテ
ィエレクトロニクス株式会社内